Generalization of the Algebraic Discrete Fourier Transform with Application to Fast Convolutions

Gabriele Steidl
Wilhelm-Pieck-Universität Rostock
Sektion Mathematik
Universitätsplatz 1
DDR-2500 Rostock, G.D.R.

Submitted by Richard A. Brualdi

ABSTRACT

By generalizing the algebraic discrete Fourier transform (ADFT) for finite commutative rings with identity, this paper opens new possibilities for combining the arithmetic in such rings, especially in residue class rings of integers $\mathbb{Z}/M\mathbb{Z}$ $(M \geqslant 2)$, with the advantages of the "classical" ADFT. The algebraic foundations for the generalization of the ADFT are prescribed, and the connection between the generalized ADFT, the minimal polynomial transform, and the so-called "reduced transform" is shown.

1. INTRODUCTION

Using polynomial arithmetic, the multiplicative complexity of cyclic convolutions and discrete Fourier transforms (DFTs) can be reduced considerably (cf. [14]). The most natural algorithm in this direction is the so-called minimal polynomial transform (MPT) (cf. [3, 11]), which is based on the Chinese remainder theorem (CRT). Unfortunately, especially with respect to hardware realizations of cyclic convolutions and DFTs, one has to apply different methods to perform the MPT and its inverse. This problem was solved on the basis of the Galois theory of fields by introducing the algebraic discrete Fourier transform (ADFT) (cf. [1–3]). The ADFT led to fast convolution algorithms due to suitable hardware implementations.

Until now it has only been possible to use the advantages of the ADFT as uniform hardware equipment for the transform and its inverse for convolu-

655 Avenue of the Americas, New York, NY 10010 0024-3795/90/$3.50

tions of sequences with components from a field. During the last few years convolutions of sequences having components in a finite commutative ring with identity have received more and more attention. This results from the fact that the arithmetic in such rings is often easy to handle. The best-known examples are residue class rings of integers modulo Fermat or Mersenne numbers, where the arithmetic is very easy to implement (cf. [11, pp. 219–220, 224–227]).

This paper generalizes the ADFT for arbitrary finite commutative rings with identity. For that, it was necessary to enlarge some tools of the Galois theory of fields, such as the normal basis concept, to special extensions of finite commutative rings with identity. These preparations are mostly contained in [12]. Some fundamental further results are prescribed in Section 3.

We show the close connection between the generalized ADFT, the MPT over finite commutative rings with identity developed in Section 4, and the so-called "reduced transform," which appears in some recent papers (cf. [5, 8, 9]). Further, we will see that the generalized ADFT has the same practically relevant properties as the "classical" ADFT. So it is distinguished from the generalized MPT and the reduced transform by uniform techniques for the transform and its inverse. Clearly, our concept includes the known ADFT over finite fields.

The generalization of the ADFT for finite commutative rings with identity opens new possibilities for the combination of the advantageous implementation of the arithmetic of such rings and special hardware implementations of the ADFT in order to provide extremely fast cyclic convolutions. A short example of the convolution of sequences with components from a ring via ADFT is demonstrated in Section 6.

2. GENERALIZED DISCRETE FOURIER TRANSFORMS

Throughout this paper, let R be a finite commutative ring with identity 1. By R^*, we denote the group of units in R. Let $N \in \mathbb{N}$ $(N \geqslant 2)$ be given. An element $e \in R$ is called a *primitive Nth root of unity in* R if

$$e^N = 1, \qquad e^j - 1 \in R^* \quad (j = 1, \ldots, N-1). \tag{2.1}$$

If $N = 1$, then $e = 1$ is said to be a primitive first root of unity in R.

THEOREM 2.1 [4]. *Let $N \in \mathbb{N}$ $(N \geqslant 2)$ be given. Then $e \in R$ is a primitive Nth root of unity in R if and only if $\Phi_N(e) = 0$ and $N \cdot 1 \in R^*$, where Φ_N denotes the Nth cyclotomic polynomial.*

If for given $N \in \mathbb{N}$ $(N \geqslant 2)$ there exists a primitive Nth root of unity $e \in R$, then R supports a generalized discrete Fourier transform of length N. In this case, the *generalized discrete Fourier transform* (GFT) *of length N over R* and its *inverse* are defined to be the following mappings between $\mathbf{y} = (y_i)_{i=0}^{N-1} \in R^N$ and $\hat{\mathbf{y}} = (\hat{y}_j)_{j=0}^{N-1} \in R^N$ [5]:

$$\begin{aligned} \hat{y}_j &:= \sum_{i=0}^{N-1} y_i e^{ij} \qquad (j = 0, \ldots, N-1), \\ y_i &:= N^{-1} \sum_{j=0}^{N-1} \hat{y}_j e^{-ij} \qquad (i = 0, \ldots, N-1). \end{aligned} \tag{2.2}$$

Note that $N^{-1} = (N \cdot 1)^{-1}$ exists by Theorem 2.1. We denote this correspondence by $\mathbf{y} \Leftrightarrow \hat{\mathbf{y}}$.

The GFT possesses properties resembling those of the classical discrete Fourier transform (DFT), particularly the *cyclic convolution property*

$$\mathbf{y} * \mathbf{z} \Leftrightarrow \hat{\mathbf{y}} \circ \hat{\mathbf{z}}, \tag{2.3}$$

where $*$ denotes the *cyclic convolution* $\mathbf{y} * \mathbf{z} = \mathbf{h} = (h_i)_{i=0}^{N-1} \in R^N$ with

$$h_i := \sum_{j=0}^{N-1} y_{|j-i|_N} z_i \qquad (j = 0, \ldots, N-1),$$

and where $\circ$ signifies the Hadamard product $\hat{\mathbf{y}} \circ \hat{\mathbf{z}} := (\hat{y}_i \hat{z}_i)_{i=0}^{N-1}$. Here $|i|_N \in \mathbb{Z}$ is the *residue of i modulo N* determined by $|i|_N \equiv i \pmod{N}$ and $0 \leqslant |i|_N < N$.

The main advantage of the GFT over the DFT is that one can replace the complex arithmetic by operations in R, for instance by the residue arithmetic modulo M $(M \geqslant 2)$ if $R := \mathbb{Z}/M\mathbb{Z}$. The resulting reduced number of multiplications and the fact that no roundoff errors occur in calculating cyclic convolutions via GFTs have inspired many authors to seek efficient methods to perform GFTs (cf. [4, 5, 8, 9]). However, a drawback of the GFT is the rigid relation between the obtainable transform length and the ring in which the transform is defined.

THEOREM 2.2 [4]. *Let R be a finite commutative ring with identity which can be decomposed into the direct sum of r local rings with the corresponding residue fields* $\mathrm{GF}(q_k)$ $(k = 1, \ldots, r)$, *where* $\mathrm{GF}(q)$ *denotes the finite field of q*

elements. Then for $N \in \mathbb{N}$, there exists a primitive Nth root of unity in R if and only if $N \mid q_k - 1$ for all $k = 1, \ldots, r$.

To overcome these restrictions on the transform length N if the signal domain R is fixed, several authors have considered GFTs over extension rings of R (cf. [5, 8, 9]). Recently, we have presented a construction method for extension rings S of a given ring R containing a primitive Nth root of unity. In the following, we summarize the results from [12] in this direction:

Assume that R can be decomposed in the direct sum of r local rings R_k with the corresponding residue fields $\mathrm{GF}(q_k)$:

$$R \cong \bigoplus_{k=1}^{r} R_k. \tag{2.4}$$

Let $N \in \mathbb{N}$ $(N \geqslant 2)$ with $\gcd(q_k, N) = 1$ $(k = 1, \ldots, r)$ be given. For $k = 1, \ldots, r$, set $d_k := \mathrm{ord}_N(q_k)$. Then by [12], $\Phi_N \in R_k[x]$ factors uniquely over R_k into $\varphi(N)/d_k$ monic basic irreducible polynomials of degree d_k, where φ signifies Euler's totient function. For the most important case $R_k := \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ (p_k prime), a constructive method for this factorization is prescribed in [12]. For a field R_k, the factorization of $\Phi_N \in R_k[x]$ into irreducible polynomials can be obtained for instance by Berlekamp's algorithm as in [7]. Assume that one basic irreducible factor $g^{(k)} \in R_k[x]$ of $\Phi_N \in R_k[x]$ $(k = 1, \ldots, r)$ is known.

As is customary, we consider the elements of the ring $\mathbb{Z}/N\mathbb{Z}$ as the integers $0, \ldots, N-1$, where addition and multiplication is performed modulo N. By $\mathbb{Z}_N^*$ we denote the multiplicative group of units in $\mathbb{Z}/N\mathbb{Z}$. Clearly, $|\mathbb{Z}_N^*| = \varphi(N)$. Let

$$U := \langle q_1, \ldots, q_r \rangle \leqslant \mathbb{Z}_N^* \tag{2.5}$$

be the *subgroup of $\mathbb{Z}_N^*$ generated by all q_k* $(k = 1, \ldots, r)$ with

$$n := |U|.$$

Further, let

$$\{c_l : l = 1, \ldots, m\}$$

with $m := \varphi(N)/n$ be a *complete set of coset representatives of U in $\mathbb{Z}_N^*$* [6, p. 39].

For $f, g \in R[x]$, where the leading coefficient of $g \in R[x]$ is a unit in R, let $|f|_g$ signify the *residue of $f \in R[x]$ modulo $g \in R[x]$*, i.e. $|f|_g \equiv f$

(mod g) and $\deg(|f|_g) < \deg(f)$ if $|f|_g \neq 0$ (cf. [6, p. 158]). Then by [12]

$$f_1^{(k)}(x) := \left| \prod_{u \in U} (x - z^u) \right|_{g^{(k)}(z)} \qquad (k = 1, \ldots, r)$$

are monic (not necessary basic irreducible) polynomials in $R_k[x]$, and

$$\Phi_N = \prod_{l=1}^{m} f_1^{(k)} \in R_k[x] \tag{2.6}$$

with

$$f_l^{(k)}(x) := \left| \prod_{u \in U} (x - z^{c_l u}) \right|_{f_l^{(k)}(z)} \qquad (k = 1, \ldots, r, \quad l = 1, \ldots, m). \tag{2.7}$$

With respect to

$$R[x] \cong \bigoplus_{k=1}^{r} R_k[x]$$

one can define the m^r polynomials $f_{l_1, \ldots, l_r} \in R[x]$ by

$$f_{l_1, \ldots, l_r} \Leftrightarrow \left(f_{l_1}^{(1)}, \ldots, f_{l_r}^{(r)} \right) \qquad (l_k = 1, \ldots, m, \quad k = 1, \ldots, r). \tag{2.8}$$

Note that for $R := \mathbb{Z}/M\mathbb{Z}$ $(M \geqslant 2)$ these polynomials can be constructed by applying the CRT [11, p. 9] to the coefficients of the corresponding polynomials $f_{l_k}^{(k)}$ $(k = 1, \ldots, r)$. Finally, we choose one of the polynomials in (2.8), for instance

$$f := f_{1,1,\ldots,1}, \tag{2.9}$$

and set

$$S := R[x]/(f) \tag{2.10}$$

with $(f) := fR[x]$. It should be noted that our construction of S is more general than in [9], where only $R := \mathbb{Z}/M\mathbb{Z}$ $(M \geqslant 2)$ is considered.

EXAMPLE 2.3. Let

$$R := \mathbb{Z}/(2^{11}-1)\mathbb{Z} \cong \mathbb{Z}/23\mathbb{Z} \oplus \mathbb{Z}/89\mathbb{Z},$$

i.e., $q_1 = 23$ and $q_2 = 89$. We represent the elements of R as symmetric residues of integers modulo $2^{11}-1$. Let $N = 8$. Then we verify that $U = \{1, 7\}$ and that $c_1 = 1$, $c_2 = 3$. Now Φ_8 factors over $\mathbb{Z}/23\mathbb{Z}$ and over $\mathbb{Z}/89\mathbb{Z}$ as follows into irreducible polynomials:

$$\Phi_8(x) = (x^2+5x+1)(x^2-5x+1) \in \mathbb{Z}/23\mathbb{Z}[x]$$

$$\Phi_8(x) = (x-12)(x+12)(x-37)(x+37) \in \mathbb{Z}/89\mathbb{Z}[x].$$

Choosing $g^{(1)}(x) := x^2+5x+1$ and $g^{(2)}(x) := x-12$, we get

$$f_1^{(1)}(x) = \left|(x-z)(x-z^7)\right|_{g^{(1)}(z)} = x^2+5x+1,$$

$$f_2^{(1)}(x) = \left|(x-z^3)(x-z^{3\cdot 7})\right|_{g^{(1)}(z)} = x^2-5x+1,$$

$$f_1^{(2)}(x) = \left|(x-z)(x-z^7)\right|_{g^{(2)}(z)} = x^2+25x+1,$$

$$f_2^{(2)}(x) = \left|(x-z^3)(x-z^{3\cdot 7})\right|_{g^{(2)}(z)} = x^2-25x+1.$$

Finally, we obtain by the CRT that one of the polynomials

$$f_{1,1}(x) = x^2-64x+1, \qquad f_{1,2}(x) = x^2-915x+1,$$

$$f_{2,1}(x) = x^2+915x+1, \qquad f_{2,2}(x) = x^2+64x+1$$

can be used for the definition of an extension ring S of R which contains a primitive 8th root of unity.

Considering S as a free R-module, we see that

$$P := \{\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}\}, \qquad \bar{x}^j := x^j + (f) \quad (j = 0, \ldots, n-1) \quad (2.11)$$

is a *polynomial basis of* S *over* R. From the definition of $f \in R[x]$ and from

(2.6) and (2.7), it follows that a factorization of $\Phi_N \in R[x]$ over R is given by

$$\Phi_N = \prod_{l=1}^{m} f_l \tag{2.12}$$

with

$$f_l(x) := \Big| \prod_{u \in U} (x - z^{c_l u}) \Big|_{f(z)} = \prod_{u \in U} (x - \bar{x}^{c_l u}) \qquad (l = 1, \ldots, m). \tag{2.13}$$

Clearly, $f_1 = f$. By Theorem 2.1, we see that $\bar{x} \in S$ is a primitive Nth root of unity in S. Hence S supports a GFT of length N which reads, by (2.2), as follows:

$$\hat{\mathbf{y}} = A_N \mathbf{y}, \qquad \mathbf{y} = A_N^{-1} \hat{\mathbf{y}}, \tag{2.14}$$

where $\mathbf{y}, \hat{\mathbf{y}} \in S^N$ and

$$A_N := (\bar{x}^{ij})_{i,j=0}^{N-1}, \qquad A_N^{-1} := N^{-1} (\bar{x}^{-ij})_{i,j=0}^{N-1}. \tag{2.15}$$

If $\mathbf{y}, \hat{\mathbf{y}} \in S^N$ are given with respect to the polynomial basis (2.11), then (2.14) coincides with the usual polynomial transform (cf. [11, pp. 155–157; 8]) of length N modulo $f \in R[x]$.

3. ON THE STRUCTURE OF SPECIAL RING EXTENSIONS

Let R as in (2.4) be the direct sum of r local rings with the corresponding residue fields $\mathrm{GF}(q_k)$. Let $N \in \mathbb{N}$ $(N \geqslant 2)$ with $\gcd(q_k, N) = 1$ $(k = 1, \ldots, s)$ be given. For any divisor $d \in \mathbb{N}$ of N, let

$$U_d := \langle q_1, \ldots, q_r \rangle \leqslant \mathbb{Z}_{N/d}^*$$

be the *subgroup of* $\mathbb{Z}_{N/d}^*$ *generated by all* q_k with

$$n_d := |U_d|.$$

In the notation of Section 2, we have $U = U_1$, $n = n_1$, and

$$U_d = \{|u|_{N/d} : u \in U\}. \tag{3.1}$$

For $i, j \in \mathbb{Z}/N\mathbb{Z}$, we introduce the equivalence relation $i \sim j$ if there exists $u \in U$ such that $j = |ui|_N$ [6, p. 88]. Let

$$T := \{t_l : l = 1, \ldots, s\}, \qquad t_1 := 1 \tag{3.2}$$

be a *set of representatives of the equivalence classes of* $\mathbb{Z}/N\mathbb{Z}$ *induced by* U. For any divisor $d \in \mathbb{N}$ of N, let

$$\{t_{d,l} : l = 1, \ldots, m_d\} \subseteq T$$

denote the *set of all elements of* T *with* $\gcd(t_{d,l}, N) = d$. Then there exist uniquely determined elements $c_{d,l} \in \mathbb{Z}^*_{N/d}$ with

$$t_{d,l} = dc_{d,l} \qquad (l = 1, \ldots, m_d). \tag{3.3}$$

It is easy to verify that these elements form a *complete set of coset representatives*

$$\{c_{d,l} : l = 1, \ldots, m_d\}$$

of U_d *in* $\mathbb{Z}^*_{N/d}$. With the notation of Section 2 it holds that $m = m_1$.

Let

$$S := R[x]/(f)$$

be defined by (2.10). Since $\bar{x} := x + (f) \in S$ is a primitive Nth root of unity in S, we have that $\bar{x}^d \in S$ is a primitive N/dth root of unity in S. Hence it follows from (2.12), (2.13), and (3.3) that

$$\Phi_{N/d} = \prod_{l=1}^{m_d} f_{d,l} \tag{3.4}$$

with

$$f_{d,l}(x) := \prod_{u \in U_d} \left(x - (\bar{x}^d)^{c_{d,l}u}\right) = \prod_{u \in U_d} (x - \bar{x}^{t_{d,l}u}). \tag{3.5}$$

Noting that every $u \in U$ can be represented in the form $u = |u|_{N/d} + j \cdot N/d$ ($j \in \mathbb{N}$), we obtain by (3.3) that

$$t_{d,l}u = c_{d,l}d(|u|_{N/d} + jN/d) = t_{d,l}|u|_{N/d} + c_{d,l}jN,$$

$$|t_{d,l}u|_N = |t_{d,l}|u|_{N/d}|_N.$$

Then by (3.1) and by the definition of our equivalence relation, (3.5) reads as

$$f_{d,l}(x) = \prod_{i \sim t_{d,l}} (x - \bar{x}^i). \tag{3.6}$$

Now we get, by

$$x^N - 1 = \prod_{d \mid N} \Phi_{N/d}(x)$$

and by (3.4) and (3.6), that

$$x^N - 1 = \prod_{d \mid N} \prod_{l=1}^{m_d} f_{d,l}(x) = \prod_{l=1}^{s} f_l(x) \tag{3.7}$$

with

$$f_l(x) := \prod_{i \sim t_l} (x - \bar{x}^i) \qquad (l = 1, \ldots, s). \tag{3.8}$$

LEMMA 3.1. *Let f_l ($l \in \{1, \ldots, s\}$) and S be given by* (3.8) *and* (2.10), *respectively. Then there exists a subring S_l of S which is isomorphic to $R[x]/(f_l)$.*

Proof. To show the assertion, we prove that

$$\tau_l : R[x]/(f_l) \to S = R[x]/(f)$$

with

$$\tau_l(a(x) + (f_l)) = a(x^{t_l}) + (f) \qquad (a \in R[x]) \tag{3.9}$$

is a monomorphism. Then

$$S_l := \operatorname{Im} \tau_l \tag{3.10}$$

is a subring of S isomorphic to $R[x]/(f_l)$.

By (3.8), it holds that $f(x) \mid f_l(x^{t_l})$. Hence we have for $a, b \in R[x]$ with $|a(x)|_{f_l} = |b(x)|_{f_l}$ that $|a(x^{t_l})|_f = |b(x^{t_l})|_f$. Using this consideration, it is easy to verify that τ is a homomorphism of $R[x]/(f_l)$ into S.

It remains to show that τ is injective. Let $d := \gcd(t_l, N)$. Assume that there exists $a(x)+(f_l) \in R[x]/(f_l)$ with $\deg(a) < \deg(f_l) = n_d$ and $a(x) \neq 0$, such that $\tau(a(x)+(f_l)) = a(x^{t_l})+(f) = (f)$, i.e. $a(\bar{x}^{t_l}) = \bar{0} \in S$, with $\bar{x} := x+(f) \in S$.

Let $\{i_1, \ldots, i_{n_d}\}$ be the set of all elements of the equivalence class of t_l. Then we obtain by the definition of S for all $j = 1, \ldots, n_d$ that

$$a(\bar{x}^{i_j}) = \bar{0}. \tag{3.11}$$

By [6, p. 159], there exists a unique polynomial $a_1 \in S[x]$, such that

$$a(x) = (x - \bar{x}^{i_1}) a_1(x),$$

which yields by (3.11) that

$$(\bar{x}^{i_j} - \bar{x}^{i_1}) a_1(\bar{x}^{i_j}) = \bar{x}^{i_1}(\bar{x}^{i_j - i_1} - 1) a_1(\bar{x}^{i_j}) = \bar{0} \qquad (j = 2, \ldots, n_d).$$

Since $\bar{x} \in S$ is a primitive Nth root of unity and $|i_j - i_1|_N \neq 0$ $(j = 2, \ldots, n_d)$, we get by (2.1) that $\bar{x}^{i_1}(\bar{x}^{i_j - i_1} - 1) \in S^*$. Thus, we have for all $j = 2, \ldots, n_d$

$$a_1(\bar{x}^{i_j}) = \bar{0}.$$

Repeating the above conclusions successively for the polynomials $a_j \in S[x]$ with

$$a_{j-1}(x) := (x - \bar{x}^{i_j}) a_j(x) \qquad (j = 2, \ldots, n_d),$$

we obtain that $\deg(a) \geqslant n_d$, which contradicts our assumption of $a \in R[x]$. Hence τ is injective. This completes the proof. ∎

For $l \in \{1, \ldots, s\}$, let S_l be given by (3.10). Let $d := \gcd(t_l, N)$. Noting that

$$P_l := \{1 + (f_l), x + (f_l), \ldots, x^{n_d - 1} + (f_l)\}$$

is a *polynomial basis* of $R[x]/(f_l)$ over R, we obtain by (3.9) that

$$\{1 + (f), x^{t_l} + (f), \ldots, x^{(n_d - 1)t_l} + (f)\} \tag{3.12}$$

is a basis of S_l over R. By [12], there exists a *group of automorphisms of* S_l *leaving* R *elementwise fixed* which is defined with respect to (3.12) by

$$\mathrm{Aut}_R S_l := \{\sigma_u : u \in U_d\}, \qquad \sigma_u(\bar{x}^{t_l}) = \bar{x}^{t_l u} = x^{t_l u} + (f).$$

Note that $\sigma_u(\sigma_v(\bar{a})) = \sigma_{uv}(\bar{a})$, $\sigma_u^{-1}(\bar{a}) = \sigma_{u^{-1}}(\bar{a})$ for all $\bar{a} \in S_l$ and all $u, v \in U_d$. If for $\bar{b} \in S_l$ the set

$$B_l := \{\sigma_u(\bar{b}) : u \in U_d\}$$

contains n_d linearly independent elements over R, then B_l is said to be a *normal basis of* S_l *over* R.

In particular we have for $S = S_1$ that

$$\mathrm{Aut}_R S := \{\sigma_u : u \in U\}, \qquad \sigma_u(\bar{x}) = \bar{x}^u = x^u + (f) \tag{3.13}$$

is an *automorphism group of* S *over* R and that for $\bar{b} \in S$

$$B := \{\sigma_u(\bar{b}) : u \in U\} \tag{3.14}$$

is a *normal basis of* S *over* R, if B consists of n linearly independent elements over R. We signify the representation of $\bar{a} \in S$ with respect to B by

$$\bar{a} = \sum_{u \in U} (\bar{a})_u \sigma_u(\bar{b}) \qquad ((a)_u \in R).$$

THEOREM 3.2 [12]. *For an extension ring* S *over* R *defined by* (2.10), *there exists a normal basis of* S *over* R.

Note that the proof of Theorem 3.2 in [12] is constructive.

For every divisor $d \in \mathbb{N}$ of N, we define a *subgroup* G_d *of* U by

$$G_d := \{g \in U : |gd|_N = d\} = \{g \in U : |g|_{N/d} = 1\}. \tag{3.15}$$

Then one can prove that for any $u, v \in U$ there exists $g \in G_d$ such that $u = vg$ if and only if $|u|_{N/d} = |v|_{N/d}$. Thus we get by (3.1) that $|U : G_d| = |U_d| = n_d$. Let

$$\{v_{d,j} : j = 1, \ldots, n_d\}$$

be a *complete set of coset representatives of* G_d *in* U. Assume that B given by (3.14) is a normal basis of S over R. Then we have, since $\bar{x} \in S$ is a primitive Nth root of unity, by (2.1), for all $g \in G_d$ and for any $t_l \in T$ with $\gcd(t_l, N) = d$,

$$\sigma_g(\bar{x}^{t_l i}) = \bar{x}^{t_l g i} = \bar{x}^{t_l i} = \sum_{u \in U} (\bar{x}^{t_l i})_u \sigma_u(\bar{b}) \qquad (i = 0, \ldots, n_d - 1).$$

On the other hand,

$$\sigma_g(\bar{x}^{t_l i}) = \sigma_g\Big(\sum_{u \in U} (\bar{x}^{t_l i})_u \sigma_u(\bar{b})\Big) = \sum_{u \in U} (\bar{x}^{t_l i})_u \sigma_{ug}(\bar{b})$$

$$= \sum_{u \in U} (\bar{x}^{t_l i})_{ug^{-1}} \sigma_u(\bar{b}) \qquad (i = 0, \ldots, n_d - 1).$$

Since B is a basis of S over R, this implies that $(\bar{x}^{t_l i})_u = (\bar{x}^{t_l i})_{ug^{-1}}$ for all $u \in U$ and all $g \in G_d$. If g runs through all elements of G_d, then $ug^{-1} \in U$ runs through all elements of that coset of G_d in U which contains u. Consequently,

$$\bar{x}^{t_j i} = \sum_{j=1}^{n_d} (\bar{x}^{t_l i})_{v_{d,j}} \bar{b}_{d,j} \qquad (i = 0, \ldots, n_d - 1) \tag{3.16}$$

with

$$\bar{b}_{d,j} := \sum_{g \in G_d} \sigma_{v_{d,j} g}(\bar{b}) \qquad (j = 1, \ldots, n_d). \tag{3.17}$$

Since the elements of B are linearly independent, the same holds for the elements of

$$B_d := \{\overline{b}_{d,j} : j = 1, \ldots, n_d\}. \tag{3.18}$$

Hence, we get by (3.12) and (3.16) that B_d is a *normal basis of* S_l *over* R for all $t_l \in T$ with $\gcd(t_l, N) = d$.

We summarize:

THEOREM 3.3. *Let* R *be given by* (2.4). *Let* $N \in \mathbb{N}$ $(N \geqslant 2)$ *with* $\gcd(q_k, N) = 1$ $(k = 1, \ldots, r)$. *Further, let* U, T, S, *and* $\mathrm{Aut}_R S$ *be defined by* (2.5), (3.2), (2.10), *and* (3.13), *respectively. Then we have for any divisor* $d \in \mathbb{N}$ *of* N:

(i) *For any* f_l *in* (3.8) *with* $\gcd(t_l, N) = d$, *there exists a subring* S_d *of* S *isomorphic to* $R[\bar{x}]/(f_l)$. *It holds that* τ_l *given by* (3.9) *is an isomorphism of* $R[x]/(f_l)$ *onto* S_d.

(ii) *There is a one-to-one correspondence between the subgroups of* U *determined by* (3.15) *and the subrings* S_d *of* S *as follows: The elements of* S_d *are elementwise fixed exactly for those automorphisms of* $\mathrm{Aut}_R S$ *belonging to the subgroup*

$$\mathrm{Aut}_{S_d} S := \{\sigma_g : g \in G_d\}$$

of $\mathrm{Aut}_R S$. *Conversely, we have that* S_d *contains all those elements of* S *which are elementwise fixed under the automorphisms of* $\mathrm{Aut}_{S_d} S$.

(iii) *If* B *in* (3.14) *is a normal basis of* S *over* R, *then* B_d *in* (3.18) *is a normal basis of* S_d *over* R.

We leave to the reader the simple proof of assertion (ii). Note that this assertion coincides with known results from the Galois theory of local rings [10, p. 301] if R is a local finite commutative ring with identity. In this case, $\mathrm{Aut}_R S$ is cyclic and for the divisors d of N, $\mathrm{Aut}_{S_d} S$ runs through all subgroups of $\mathrm{Aut}_R S$. The later is not true for arbitrary finite commutative rings with identity.

4. FAST CYCLIC CONVOLUTIONS VIA CRT

Let R as in (2.4) be the direct sum of r local rings with the corresponding residue fields $\mathrm{GF}(q_k)$ $(k = 1, \ldots, r)$. Let $N \in \mathbb{N}$ $(N \geqslant 2)$ with $\gcd(q_k, N)$

$= 1$ $(k = 1, \ldots, r)$ be given. Let U be the subgroup (2.5) of $\mathbb{Z}_N^*$, and let

$$T := \{t_l : l = 1, \ldots, s\}, \qquad t_1 := 1,$$

be a set of representatives of the equivalence classes of $\mathbb{Z}/N\mathbb{Z}$ induced by U. We define a polynomial $f \in R[x]$ by (2.9) and the extension ring $S := R[x]/(f)$ of R by (2.10). Further, we introduce the polynomials f_l $(l = 1, \ldots, s)$ as in (3.8).

For the rest of this paper, we consider the elements of $R[x]/(f_l)$ $(l = 1, \ldots, s)$, in particular the elements of S, as polynomials $a \in R[x]$ with $\deg(a) < \deg(f_l)$ for $a(x) \neq 0$, where all calculations are performed modulo f_l.

For $j, l \in \{1, \ldots, s\}$ with $j \neq l$, it holds that $(f_j) + (f_l) = R[x]$, which implies by (3.7) and [6, p. 132] that

$$R[x]/(x^N - 1) \cong \bigoplus_{l=1}^{s} R[x]/(f_l).$$

Now we obtain by the CRT [6, p. 131]:

If $y^{(l)} \in R[x]$ with $\deg(y^{(l)}) < \deg(f_l)$ $(l = 1, \ldots, s)$ are given, then there exists a polynomial $y \in R[x]$ of degree less than N which is uniquely determined by $|y|_{f_l} = y^{(l)}$ $(l = 1, \ldots, s)$.

By [12], we notice two different methods, called *Chinese remainder reconstructions*, to produce such a polynomial $y \in R[x]$ from given $y^{(l)} \in R[x]$:

(1) $y(x) = |\sum_{l=1}^{s} (x^N - 1) y^{(l)}(x) f_l'(x)/f_l(x)|_{x^N - 1}$, where $f_l' \in R[x]$ is determined by $|(x^N - 1) f_l'(x)/f_l(x)|_{f_l} = 1$ $(l = 1, \ldots, s)$.

(2) $y = [y^{(1)}] + [y^{(1)} y^{(2)}] f_1 + \cdots + [y^{(1)} \cdots y^{(s)}] f_1 \cdots f_{s-1}$ with *modular divided differences* $[y^{(l)}] := y^{(l)}$ $(l = 1, \ldots, s)$, $[y^{(j)} y^{(l)}] := |([y^{(l)}] - [y^{(j)}]) f_j^{-1}|_{f_l}$ $(1 \leqslant j < l \leqslant s)$,

$$\left[y^{(l_1)} \cdots y^{(l_{i-1})} y^{(l_i)}\right] := \left| \left(\left[y^{(l_1)} \cdots y^{(l_{i-2})} y^{(l_i)}\right] - \left[y^{(l_1)} \cdots y^{(l_{i-1})}\right] \right) f_{l_{i-1}}^{-1} \right|_{f_{l_i}}$$

$(1 \leqslant l_1 < \cdots < l_i \leqslant s)$, where $|f_j^{-1}|_{f_l} \in R[x]$ $(j \neq l)$ is determined by $|f_j f_j^{-1}|_{f_l} = 1$.

Let

$$y(x) := \sum_{i=0}^{N-1} y_i x^i \in R[x] \tag{4.1}$$

be the *associated polynomial of* $\mathbf{y} = (y_i)_{i=0}^{N-1} \in R^N$. We call the map of R^N onto $\oplus_{l=1}^{s} R[x]/(f_l)$ defined by

$$\mathbf{y} \to (y^{(l)})_{l=1}^{s}, \quad y^{(l)} := |y|_{f_l} \qquad (l = 1, \ldots, s) \tag{4.2}$$

the *minimal polynomial transform* (MPT) of $\mathbf{y} \in R^N$. It can be considered as a generalization of the usual MPT (cf. [3]) of sequences with components from a field. The MPT is a bijection, and its inverse can be calculated by Chinese remainder reconstructions.

Now one can design an algorithm for the cyclic convolution $\mathbf{h} = \mathbf{y} * \mathbf{z}$ of sequences $\mathbf{y}, \mathbf{z} \in R^N$.

ALGORITHM 1.

1. Calculate $(y^{(l)})_{l=1}^{s}$ and $(z^{(l)})_{l=1}^{s}$ via the MPT (4.2).
2. Compute the polynomial products $h^{(l)} := |y^{(l)} \cdot z^{(l)}|_{f_l}$ $(l = 1, \ldots, s)$.
3. Calculate $\mathbf{h}$ from $(h^{(l)})_{l=1}^{s}$ by the Chinese remainder reconstruction and by (4.1).

Algorithm 1 coincides with the usual convolution algorithm based on the CRT (cf. [11, pp. 35–37]) if R is a field. Note that there exist efficient methods to perform step 2 of Algorithm 1 (cf. [11, pp. 73–78; 13]).

Using (2.3), we are led to another algorithm to calculate cyclic convolutions of N-point sequences with components from R based on the GFT over S. Unfortunately, this approach extends the R-arithmetic to the more expensive arithmetic in S. One compromise which decreases the computational complexity of convolutions via GFTs makes use of the so-called *conjugate symmetry property* [5]: Let an automorphism group $\mathrm{Aut}_R S$ of S over R be given by (3.13). For $\mathbf{y} \in R^N$, let $\hat{\mathbf{y}} \in S^N$ be defined by (2.14). Then it holds for all $w \in U$ that

$$\sigma_w(\hat{y}_j) = \sigma_w\left(\sum_{i=0}^{N-1} y_i x^{ij}\right) = \sum_{i=0}^{N-1} y_i x^{ijw} = \hat{y}_{|jw|_N}. \tag{4.3}$$

Hence, by the definition of our equivalence relation, the GFT of $\mathbf{y} \in R^N$ is

determined by $(\hat{y}_{t_l})_{l=1}^{s} \in S^s$. The GFT which calculates exactly the representatives $\hat{y}_{t_l}$ $(l = 1, \ldots, s)$ of the components of $\hat{\mathbf{y}} \in S^N$ is called the *reduced GFT of length N over S*. The following convolution algorithm to obtain $\mathbf{h} = \mathbf{y} * \mathbf{z}$ for $\mathbf{y}, \mathbf{z} \in R^N$ via the reduced GFT was developed in [9].

ALGORITHM 2.

1. Calculate $(\hat{y}_{t_l})_{l=1}^{s}$ and $(\hat{z}_{t_l})_{l=1}^{s}$ via the reduced GFT using (2.14).
2. Compute $(\hat{h}_{t_l})_{l=1}^{s} := (\hat{y}_{t_l} \cdot \hat{z}_{t_l})_{l=1}^{s}$ with respect to P.
3. Arrange $\hat{\mathbf{h}}$ from $(\hat{h}_{t_l})_{l=1}^{s}$ by (4.3), and calculate $\mathbf{h}$ via the inverse GFT (2.14).

It has been shown that the reduced GFT is the basis of many known efficient convolution techniques (cf. [9]). By (2.15) and (3.9), we get the following rigid relation between the MPT and the reduced GFT of $\mathbf{y} \in R^N$:

$$\hat{y}_{t_l} = \left| y^{(l)}(x^{t_l}) \right|_f \qquad (l = 1, \ldots, s). \tag{4.4}$$

For $l \in \{1, \ldots, s\}$ with $\gcd(t_l, N) = d$, let

$$\left(\left| x^{t_l j} \right|_f \right)_{j=0}^{n_d - 1} = A_l' (x^i)_{i=0}^{N-1}, \qquad A_l := \left(a_{ij}^{(l)} \right)_{i,j=0}^{N-1, n_d - 1},$$

where A_l' denotes the transpose of A_l. Assume that

$$\hat{y}_{t_l}(x) := \sum_{i=0}^{N-1} \hat{y}_{t_l, i} x^i \in S, \qquad y^{(l)}(x) := \sum_{j=0}^{n_d - 1} y_j^{(l)} x^j \in R[x]/(f_l) \tag{4.5}$$

are given with respect to the polynomial bases in $S := R[x]/(f)$ and in $R[x]/(f_l)$ $(l = 1, \ldots, s)$, respectively. Then (4.4) reads as

$$(\hat{y}_{t_l, i})_{i=0}^{N-1} = A_l \left(y_j^{(l)} \right)_{j=0}^{n_d - 1}. \tag{4.6}$$

By Lemma 3.1, the (N, n_d)-matrix A_l has rank n_d. Hence, one can conversely obtain $y^{(l)}$ from given $\hat{y}_{t_l}$ by the unique solution $(y_j^{(l)})_{j=0}^{n_d - 1}$ of (4.6) and by (4.5). This answers open questions on the connection between factorizations of $x^N - 1 \in R[x]$ over R and the reduced GFT in [9].

With respect to software and hardware realizations of convolutions, the reduced GFT has the disadvantage that its inverse transform cannot be reduced by the conjugate symmetry property, since the input sequences for

the inverse GFT have in general components in S. Similarly, the algorithm for the MPT (4.2) differs from the Chinese remainder reconstruction which is necessary to perform the inverse MPT.

In the following, we overcome this drawback of both convolution algorithms by introducing a new transform using the normal basis of S. This idea is based on [1–3], where the question if the MPT of sequences with components from a field and its inverse can be performed with the same kind of equipment was solved by connecting the MPT with the normal basis of fields.

5. THE ALGEBRAIC DISCRETE FOURIER TRANSFORM

Let R as in (2.4) be the direct sum of r local rings with the corresponding residue fields $\mathrm{GF}(q_k)$ $(k = 1,\dots,r)$. Let $N \in \mathbb{N}$ $(N \geqslant 2)$ with $\gcd(q_k, N) = 1$ $(k = 1,\dots,r)$ be given. Let U be the subgroup of $\mathbb{Z}_N^*$ generated by all q_k, and let

$$T := \{t_l : l = 1,\dots,s\}, \qquad t_1 := 1$$

be a set of representatives of the equivalence classes of $\mathbb{Z}/N\mathbb{Z}$ induced by U. We define a polynomial $f \in R[x]$ by (2.9) and the extension ring $S := R[x]/(f)$ of R by (2.10). Further, we introduce $\mathrm{Aut}_R S$ as in (3.13). Let

$$B := \{\sigma_u(b) : u \in U\} \tag{5.1}$$

be a normal basis of S over R.

We consider the components of the image $\hat{\mathbf{y}} \in S^N$ of the GFT (2.14) of $\mathbf{y} \in R^N$. By (2.15), we have

$$(\hat{y}_j)_u = \sum_{i=0}^{N-1} y_i (x^{ij})_u \qquad (u \in U). \tag{5.2}$$

Now the conjugate symmetry property (4.3) reads for all $w \in U$ as follows:

$$\begin{aligned} \sigma_w(\hat{y}_{t_l}) &= \sigma_w\Big(\sum_{u \in U} (\hat{y}_{t_l})_u \sigma_u(b)\Big) = \sum_{u \in U} (\hat{y}_{t_l})_u \sigma_{uw}(b) \\ &= \sum_{u \in U} (\hat{y}_{t_l})_{uw^{-1}} \sigma_u(b) = \hat{y}_{|t_l w|_N} \qquad (l = 1,\dots,s). \end{aligned} \tag{5.3}$$

This implies for all $w \in U$ that

$$\left(\hat{y}_{|t_l w|_N}\right)_u = \left(\hat{y}_{t_l}\right)_{uw^{-1}} \qquad (u \in U). \tag{5.4}$$

Hence, the whole image $\hat{\mathbf{y}} \in S^N$ of $\mathbf{y} \in R^N$ can be obtained with respect to B by simple shifts of the coefficients of $\hat{y}_{t_l} \in S$ $(l = 1, \ldots, s)$ in the representation (5.2).

Now we generalize the ADFT [1, p. 252] for finite commutative rings with identity. The *algebraic discrete Fourier transform* (ADFT) *of length N over R* is defined to be the following mapping between $\mathbf{y} = (y_i)_{i=0}^{N-1} \in R^N$ and $\mathbf{Y} = (Y_j)_{j=0}^{N-1} \in R^N$:

$$\mathbf{Y} := B_{A_N}\mathbf{y}, \qquad B_{A_N} := \left((x^{ij})_1\right)_{i,j=0}^{N-1}, \tag{5.5}$$

where $(x^{ij})_1$ denotes the coefficient of $\sigma_1(b) = b$ in the representation of $x^{ij} \in S$ with respect to B. The connection between the ADFT and the reduced GFT is given by

THEOREM 5.1. *Under the above assumptions, the ADFT of* $\mathbf{y} \in R^N$ *determines the components* $\hat{y}_{t_l}$ $(l = 1, \ldots, s)$ *of* $\hat{\mathbf{y}} \in S^N$ *defined by* (2.14) *with respect to the normal basis B.*

Proof. Assume that $\mathbf{Y} \in R^N$ is calculated by (5.6). Let $l \in \{1, \ldots, s\}$ with $d = \gcd(t_l, N)$. For the subgroup G_d of U in (3.15), let

$$\{v_{d,j} : j = 1, \ldots, n_d\}$$

be a complete set of coset representatives of G_d in U. Then it holds by (2.15) and (3.16) that

$$\hat{y}_{t_l} = \sum_{j=1}^{n_d} \left(\hat{y}_{t_l}\right)_{v_{d,j}} b_{d,j}, \tag{5.6}$$

with $b_{d,j}$ $(j = 1, \ldots, n_d)$ defined by (3.17). Set

$$k_{l,j} := \left|t_l v_{d,j}^{-1}\right|_N \qquad (j = 1, \ldots, n_d).$$

Then we obtain by (5.5), (5.2), and (5.4) that

$$Y_{k_{l,j}} = \sum_{i=0}^{N-1} y_i (x^{k_{l,j} i})_1 = (\hat{y}_{t_l})_{v_{d,j}} \qquad (j = 1, \ldots, n_d).$$

Consequently, we conclude by (5.6) that

$$\hat{y}_{t_l} = \sum_{j=1}^{n_d} Y_{k_{l,j}} b_{d,j}. \tag{5.7}$$

This completes the proof. ■

On the other hand, it follows from the above proof that one can reconstruct $\mathbf{Y}$ from $\hat{y}_{t_l}$ $(l = 1, \ldots, s)$ by

$$Y_{k_{1,j}} = (\hat{y}_{t_l})_{v_{d,j}} \qquad (l = 1, \ldots, s; \quad j = 1, \ldots, n_d). \tag{5.8}$$

Let the polynomials $f_l \in R[x]$ $(l = 1, \ldots, s)$ be given by (3.8). For any divisor $d \in \mathbb{N}$ of N, let the subring S_d of S be defined by Theorem 3.3(i). For $l \in \{1, \ldots, s\}$ with $d = \gcd(t_l, N)$, we denote by

$$Q_l := \left(q_{ij}^{(l)}\right)_{i,j=1}^{n_d}$$

the matrix of the automorphism of S_d relative to the ordered bases $\{x^{t_l(j-1)}: j = 1, \ldots, n_d\}$ and $\{b_{d,j}: j = 1, \ldots, n_d\}$ of S_d over R, i.e.

$$\left(|x^{t_l(j-1)}|_f\right)_{j=1}^{n_d} = Q_l^t \left(b_{d,j}\right)_{j=1}^{n_d}.$$

Assume that

$$y^{(l)}(x) = \sum_{j=1}^{n_d} y_{j-1}^{(l)} x^{j-1}, \qquad \hat{y}_{t_l} = \sum_{j=1}^{n_d} Y_{k_{l,j}} b_{d,j}.$$

Then we obtain by (2.15) and by Lemma 3.1 the following relation between the MPT (4.2) and the ADFT (5.6) of $\mathbf{y} \in R^N$:

$$\left(Y_{k_{l,j}}\right)_{j=1}^{n_d} = Q_l \left(y_{j-1}^{(l)}\right)_{j=1}^{n_d}. \tag{5.9}$$

Figure 1 gives the first complete description of the connection between the GFT, the reduced GFT, the MPT, and the ADFT of $\mathbf{y} \in R^N$.

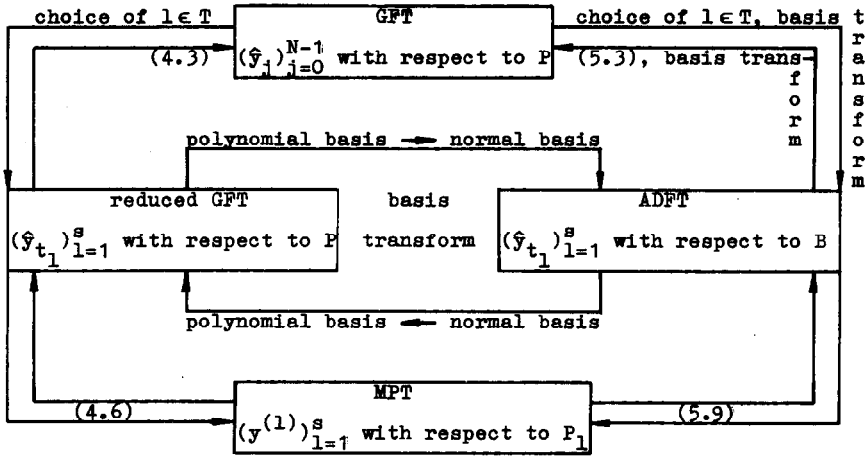

FIG. 1. Connection between GFT, reduced GFT, ADFT, and MPT of $y \in R^N$.

To define the inverse ADFT, we need further preliminaries. We introduce the *trace of* $a = a(x) \in S$ *over* R by

$$\operatorname{tr}(a(x)) := \sum_{u \in U} \sigma_u(a(x)) = \sum_{u \in U} a(x^u).$$

By [12], the trace function is an R-linear map of S onto R.

Two bases $B := \{b_0, \ldots, b_{n-1}\}$ and $C := \{c_0, \ldots, c_{n-1}\}$ of S over R are called *dual bases* if $\operatorname{tr}(b_i c_j) = \sigma_{ij}$ for all $i, j = 0, \ldots, n-1$, where σ_{ij} is the Kronecker symbol. If $\operatorname{tr}(b_i b_j) = \sigma_{ij}$ or $\operatorname{tr}(b_i b_{\pi(j)}) = \sigma_{ij}$ for all $i, j = 0, \ldots, n-1$, where π signifies a permutation of $0, \ldots, n-1$, then B is said to be a *self-dual basis of* S *over* R or a *weak self-dual basis of* S *over* R, respectively.

We enumerate the elements of U by $u_0 = 1, u_1, \ldots, u_{n-1}$. For $A := \{a_0, \ldots, a_{n-1}\}$ $(a_i \in S)$, set

$$D_{\sigma,A} := \left(\sigma_{u_j}(a_i)\right)_{i,j=0}^{n-1} \in S^{n \times n},$$

$$D_A := \left(\operatorname{tr}(a_i a_j)\right)_{i,j=0}^{n-1} \in R^{n \times n}.$$

Note that $D_{\sigma,A} D'_{\sigma,A} = D_A$.

THEOREM 5.1 [12]. *Let R and S be given by* (2.4) *and* (2.10), *respectively. Let $B := \{b_0, \ldots, b_{n-1}\}$ be any basis of S over R. Then*:

(i) *The matrices $D_{\sigma,B}$ and D_B are invertible in $S^{n\times n}$ and in $R^{n\times n}$, respectively.*

(ii) *There exists a unique dual basis $C := \{c_0, \ldots, c_{n-1}\}$ of B determined by*

$$(c_0, \ldots, c_{n-1})' = D_B^{-1}(b_0, \ldots, b_{n-1})'.$$

It holds that $D_B^{-1} = D_C$, $D_{\sigma,B}^{-1} = D'_{\sigma,C}$. Consequently, C is given by the first column of $D_{\sigma,B}^{-1}$, too.

(iii) *If B is a normal basis of S over R, then the dual basis of B is also a normal basis of S over R.*

In the following, let

$$C := \{\sigma_u(c) : u \in U\}$$

be the dual basis of the normal basis B in (5.1).

THEOREM 5.2. *The generalized ADFT over R is a bijection. The inverse generalized ADFT over R is defined to be the following mapping between $\mathbf{Y} \in R^N$ and $\mathbf{y} \in R^N$:*

$$\mathbf{y} = C_{A_N^{-1}}\mathbf{Y}, \qquad C_{A_N^{-1}} := N^{-1}\big((x^{-ij})_1\big)_{i,j=0}^{N-1}, \tag{5.10}$$

where $(x^{-ij})_1$ denotes the coefficient of $\sigma_1(c) = c$ in the representation of $x^{-ij} \in S$ with respect to C.

Proof. By definition of the dual basis, it holds that

$$B_{A_N} = \big(\mathrm{tr}(x^{ij}c)\big)_{i,j=0}^{N-1}, \qquad C_{A_N^{-1}} = N^{-1}\big(\mathrm{tr}(x^{-ij}b)\big)_{i,j=0}^{N-1}.$$

Hence, we obtain for $(r_{ij})_{i,j=0}^{N-1} := B_{A_N} \cdot C_{A_N^{-1}}$ that

$$r_{ij} = N^{-1} \sum_{k=0}^{N-1} \operatorname{tr}(x^{ik}c) \operatorname{tr}(x^{-jk}b)$$

$$= N^{-1} \sum_{k=0}^{N-1} \left(\sum_{u \in U} \sigma_u(x^{ik}c) \right) \left(\sum_{v \in U} \sigma_v(x^{-jk}b) \right)$$

$$= N^{-1} \sum_{u \in U} \sum_{v \in U} \left(\sum_{k=0}^{N-1} x^{(iu-jv)k} \right) \sigma_u(c)\sigma_v(b).$$

Since $x \in S$ is a primitive Nth root of unity, the inner sum vanishes by [4] in the case that $|iu|_N \neq |jv|_N$. Thus,

$$r_{ij} = \begin{cases} 0 & \text{if} \quad j \neq iuv^{-1}, \\ \sum_{u \in U} \sum_{v \in U} \sigma_u(c)\sigma_v(b) & \text{otherwise.} \end{cases}$$

If $j = iuv^{-1}$, then we verify that

$$r_{ij} = \sum_{u \in U} \sum_{\substack{v \in U \\ j = iv}} \sigma_u(c)\sigma_{uv^{-1}}(b).$$

Since B and C are dual bases of S over R, this implies that

$$r_{ij} = \sum_{\substack{v \in U \\ j = iv}} \operatorname{tr}(c\sigma_{v^{-1}}(b)) = \begin{cases} 0, & \text{if} \quad i \neq j, \\ 1 & \text{otherwise,} \end{cases}$$

and we have finished the proof. ∎

We summarize: The ADFT over R is defined for any transform length N with $\gcd(q_k, N) = 1$ $(k = 1, \ldots, r)$. For example, one can perform ADFTs of great length in residue class rings of integers modulo Fermat or Mersenne numbers. If $N \mid q_k - 1$ for all $k = 1, \ldots, r$, then the ADFT coincides with the usual GFT of length N over R.

Necessary preparations for the ADFT are the construction of an extension ring S of R of the form (2.10) and of a normal basis B of S over R. Then the ADFT and its inverse can be computed via similar algorithms. By (5.5) and

(5.10), it is desirable to choose B as a self-dual or as a weak self-dual basis. Here, we refer to [12].

The ADFT can be performed only with R-arithmetic, for some ring R and transform length N without multiplications. By the special structure of the GFT matrix A_N, there can be deduced fast algorithms for the ADFT like the Rader algorithm or composite algorithms [11, pp. 116–120; 1, pp. 211–224] (see Example 6.1). Some other known DFT algorithms are only applicable under additional assumptions.

The ADFT can be computed by the reduced GFT or by the MPT and by postconverting the outputs according to the normal basis B. Similarly, the inverse ADFT can be performed by means of these transforms, but here the output values have to be represented with respect to the dual basis C of B.

On the other hand, the normal basis concept yields a possibility of calculating reduced GFTs or MPTs and their inverses via uniform algorithms at the cost of precomputing the input data of the inverse transforms with respect to B and postcomputing the output values with respect to C (see Figure 1).

The whole image $\hat{\mathbf{y}} \in S^N$ of $\mathbf{y} \in R^N$ can be obtained with respect to B from $\mathbf{Y} \in R^N$ by (5.7) and by simple shifts (5.3).

6. CYCLIC CONVOLUTIONS VIA ADFT's

Let R be given by (2.4). Let $N \in \mathbb{N}$ $(N \geqslant 2)$ with $\gcd(q_k, N) = 1$ $(k = 1, \ldots, r)$. We define U and T by (2.5) and (3.2), respectively. Further, we introduce an extension ring $S := R[x]/(f)$ of R by (2.10). Let $\mathrm{Aut}_R S$ be the automorphism group (3.13) of S over R. Finally, assume that $B := \{\sigma_u(b) : u \in U\}$ and $C := \{\sigma_u(c) : u \in U\}$ are dual normal bases of S over R.

By $\hat{\mathbf{y}} \in S^N$ and $\mathbf{Y} \in R^N$, we denote the GFT (2.14) and the ADFT (5.5) of $\mathbf{y} \in R^N$, respectively. Then one can deduce the following algorithm for the convolution $\mathbf{h} = \mathbf{y} * \mathbf{z}$ of $\mathbf{y}, \mathbf{z} \in R^N$:

Algorithm 3.

1. Calculate $\mathbf{Y}$ and $\mathbf{Z}$ via the ADFT (5.5), and arrange $(\hat{y}_{t_l})_{l=1}^{s}$ and $(\hat{z}_{t_l})_{l=1}^{s}$ with respect to B by (5.7).
2. Compute $(\hat{h}_{t_l})_{l=1}^{s} = (\hat{y}_{t_l} \cdot \hat{z}_{t_l})_{l=1}^{s}$ with respect to B.
3. Arrange $\mathbf{H}$ from $(\hat{h}_{t_l})_{l=1}^{s}$ by (5.8), and calculate $\mathbf{h}$ via the inverse ADFT (5.10).

By Figure 1, there are several possibilities for replacing the steps in Algorithm 3 by similar steps of Algorithm 1 or 2. However, in contrast with

these algorithms, the ADFT in step 1 of Algorithm 3 and its inverse in step 3 can be calculated by the same procedure. This property has been used for special fast hardware realizations of convolutions of sequences with components from a field (cf. [1–3]). Now one can extend these considerations to the more general case that the signal domain is a finite commutative ring with identity. This will be interesting especially in connection with residue class rings of integers modulo Fermat or Mersenne numbers.

Considering step 2 of Algorithm 3, we mention that there exist special techniques for the multiplication of elements in S with respect to a normal basis B (cf. [1, pp. 263–268]).

EXAMPLE 6.1. The task is to convolve the 8-point sequences

$$\mathbf{y} = (2,0,1,-3,5,-1,7,0)', \qquad \mathbf{z} = (-7,-2,0,1,1,-5,-4,1)'$$

over $R := \mathbb{Z}/(2^{11}-1)\mathbb{Z}$. Since $2^{11}-1$ is a Mersenne number, R possesses a simple arithmetic. In particular, multiplications by powers of 2 can be realized as bit rotations (cf. [11, pp. 219–220]).

We use Example 2.3. We choose $T = \{t_1 = 1, t_2 = 3, t_3 = 2, t_4 = 4, t_5 = 0\}$ as set of representatives of the equivalence classes of $\mathbb{Z}/8\mathbb{Z}$ induced by $U = \{1,7\}$. Set $S := R[x]/(f)$ with $f(x) := x^2 - 64x + 1$. Then

$$B := \{b_0 = 37x,\ b_1 = 37x^7 = -32x + 1\}$$

is a weak self-dual normal basis of S over R, and we have for the polynomial basis $P = \{1, x\}$ of S over R

$$1 = b_0 + b_1, \qquad x = 64b_0. \tag{6.1}$$

Now $b_{1,1} = b_{2,1} = b_0$, $b_{1,2} = b_{2,2} = b_1$, $b_{4,1} = b_{8,1} = b_0 + b_1 = 1$, and $k_{l,1} = t_l$ $(l = 1,\ldots,5)$, $k_{l,2} = |7t_l|_8$ $(l = 1,2,3)$. In order to apply a Rader-like algorithm for the ADFT similar to that in [1, pp. 220–224; 11, pp. 118–120], we use $\tilde{B}_{A_N}$, $\tilde{C}_{A_N^{-1}}$ instead of B_{A_N}, $C_{A_N^{-1}}$, respectively. These matrices can be obtained from B_{A_N} and $C_{A_N^{-1}}$ by the permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 4 & 2 & 7 & 1 & 5 & 3 & 6 \end{pmatrix}$$

of their rows and columns; i.e., by (5.5), (5.10), and (6.1),

$$\tilde{B}_{A_N} := \begin{array}{c} \begin{matrix} 0 & 4 & 2 & 6 & 1 & 5 & 7 & 3 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 64 & -64 & 0 & 0 \\ 1 & -1 & 1 & -1 & -64 & 64 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 & 64 & -64 \\ 1 & -1 & -1 & 1 & 0 & 0 & -64 & 64 \end{pmatrix} \end{array} \begin{matrix} 0 \\ 4 \\ 2 \\ 6 \\ 1' \\ 5 \\ 7 \\ 3 \end{matrix}$$

$$\tilde{C}_{A_N^{-1}} := 256 B_{A_N}.$$

Then the ADFT of length 8 over R requires 22 additions and 2 shifts.

Now Algorithm 3 reads for the given sequences $\mathbf{y}$, $\mathbf{z}$ as follows:

1. $\mathbf{Y} = (11, 55, 1, -189, 19, -73, -3, 195)'$,
   $\mathbf{Z} = (-15, 188, -11, -12, -5, -196, 7, -12)'$,
   $\hat{y}_0 = 11$, $\hat{z}_0 = -15$, $\hat{y}_4 = 19$, $\hat{z}_4 = -5$,
   $\hat{y}_2 = b_0 - 3b_1$, $\hat{z}_2 = -11b_0 + 7b_1$,
   $\hat{y}_1 = 55b_0 + 195b_1$, $\hat{z}_1 = 118b_0 - 12b_1$,
   $\hat{y}_3 = 189b_0 - 73b_1$, $\hat{z}_3 = -12b_0 - 196b_1$.
2. $\hat{h}_0 = 165$, $\hat{h}_4 = -95$, $\hat{h}_2 = 25b_0 + 15b_1$,
   $\hat{h}_1 = -224b_0 - 622b_1$, $\hat{h}_3 = 658b_0 + 416b_1$.
3. $\mathbf{H} = (165, -224, 25, 658, -95, 416, 15, -622)'$,
   $\mathbf{h} = (554, 543, 535, 548, 497, 548, 496, 538)'$.

REFERENCES

1 T. Beth, *Verfahren zur Schnellen Fourier-Transformation*, Teubner-Studienbücherei Informatik, Stuttgart, 1984.

2 T. Beth, W. Fumy, and R. Mühlfeld, Zur algebraischen diskreten Fourier-Transformation, *Arch. Math. (Basel)* 40:238–244 (1983).

3 T. Beth and W. Fumy, Hardware-oriented algorithms for the fast symbolic calculation of the DFT, *Electron. Lett.* 19(21):901–902 (1983).

4 R. Creutzburg and M. Tasche, *F*-Transformationen und Faltungen in kommutativen Ringen, *Elektron. Informationsverarb. Kybernet.* 22:129–149 (1985).

5 E. Dubois and A. N. Venetsanopoulos, Convolutions using a conjugate symmetry property for the generalized discrete Fourier transform, *IEEE Trans. Acoust. Speech Signal Process.* 26(2):165–170 (1978).

6 T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
7 H. Lüneburg, *On a Rational Normal Form of Endomorphisms*, BI-Wissenschaftsverlag, Mannheim, 1988.
8 J. B. Martens and M. C. Vanwormhoudt, Convolutions using a conjugate symmetry property for number theoretic transforms over rings of regular integers, *IEEE Trans. Acoust. Speech Signal Process.* 31(5):1121–1124 (1983).
9 J. B. Martens and M. C. Vanwormhoudt, Convolutions of long integer sequences by means of number theoretic transforms over residue class polynomial rings, *IEEE Trans. Acoust. Speech Signal Process.* 31(5):1125–1134 (1983).
10 B. R. McDonalds, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.
11 H. J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms*, Springer-Verlag, Berlin, 1981.
12 G. Steidl, On normal bases for finite commutative rings, *Math. Nachr.*, to appear.
13 S. Winograd, Some bilinear forms whose multiplicative complexity depends on the field of constants, *Math. Systems Theory* 10:169–180 (1977).
14 S. Winograd, On computing the discrete Fourier transform, *Math. Comp.* 32/(141):175–199 (1978).

Received 28 December 1988; final manuscript accepted 21 July 1989